

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF SOUTH CAROLINA
COLUMBIA DIVISION**

**IN RE: BLACKBAUD, INC.,
CUSTOMER DATA SECURITY
BREACH LITIGATION**

Case No. 3:20-mn-02972-JFA

MDL No. 2972

ORDER AND OPINION

THIS DOCUMENT RELATES TO: ALL ACTIONS:

This matter is before the court on motions by both Plaintiffs and Defendant to have the court determine which state’s common law principles will apply to the substantive claims asserted in this case. (ECF Nos. 252–255). Specifically, Plaintiffs seek to have South Carolina law applied to the common law claims of negligence, negligence per se, and invasion of privacy; meanwhile, Blackbaud moves to have the law of each state where a respective plaintiff is domiciled to apply to those specific common law claims. *Id.* This matter has been fully briefed and is ripe for review.

I. FACTUAL BACKGROUND

Blackbaud, Inc., a cloud-based services provider, is a publicly traded company incorporated in Delaware and headquartered in Charleston, South Carolina. (ECF No. 77 at ¶¶ 419, 424). The company provides data collection and maintenance software solutions for administration, fundraising, marketing, and analytics for “social good entities.”¹ *Id.* at ¶¶ 4, 430. Blackbaud’s services include collecting and storing personally identifiable

¹ The social good entities include cultural organizations, foundations, educational institutions, faith communities, and healthcare organizations (hereinafter, “Social Good Entities”). *Id.*

information and personal health information (“Personal Information” or “PI”) about the Social Good Entities’ donors, students, congregants, and patients. *Id.* at ¶¶ 2, 429.

Plaintiffs represent a putative class of individuals whose Personal Information was provided to Blackbaud’s customers (the Social Good Entities) and managed by Blackbaud. *Id.* at ¶ 12. Plaintiffs are not Blackbaud’s direct customers, but the patrons of the Social Good Entities that are direct customers of Blackbaud. (ECF Nos. 92-1 & 109). Plaintiffs allege that cybercriminals orchestrated a ransomware style data breach attack from February 7, 2020 to May 20, 2020. (ECF No. 77 at ¶ 25). Blackbaud ultimately paid the ransom in exchange for a commitment that any data previously accessed by the cybercriminals be permanently destroyed. (ECF Nos. 77 at ¶ 20; 138 at ¶ 499; & 92-1). Plaintiffs allege that Blackbaud’s security program was inadequate and that the security risks associated with the Personal Information went unmitigated, allowing the cybercriminals to gain access. (ECF No. 77 at ¶ 439). During the subsequent discovery, Blackbaud stated that its domestic data centers are located in Massachusetts, Texas, California, and New Jersey. (ECF No. 254 at 3). Blackbaud further contends, apparently without contradictions, that the servers which house the Plaintiffs data—and the initial point of entry for the ransomware attack—are physically located in Massachusetts. *Id.* at 3-4.

II. PROCEDURAL BACKGROUND

Prior to the instant motion, both Parties asserted choice of law arguments within the context of Blackbaud’s motion to dismiss. (ECF Nos. 124-1 & 142-1). Both parties have agreed that South Carolina choice of law principles apply in this action. (ECF No. 93).

Thus, “[u]nder traditional South Carolina choice of law principles, the substantive law governing a tort action is determined by the *lex loci delicti*, the law of the state in which the [alleged] injury occurred.” *Boone v. Boone*, 345 S.C. 8, 13, 546 S.E.2d 191, 193 (2001).

In briefing Blackbaud’s prior motion to dismiss, Blackbaud and Plaintiffs argued their respective positions on the place of injury. Blackbaud argued that the law of the state where a Plaintiff resides should apply to that specific Plaintiff’s common law tort claims. (ECF No. 124-1 at 7-8). In response, Plaintiffs moved that South Carolina law should be applied based on Blackbaud’s decisions related to “security measures” and “all of Plaintiffs’ tort claims arise out of Blackbaud’s failure to implement security measures to protect Plaintiffs’ Personal Information.” (ECF No. 142-1 at 4-5).

In contravention of both parties’ stated arguments, the court² held that “the original point of intrusion—that is how the data breach began in the first instance,” was the critical fact under the *lex loci delicti* analysis per South Carolina choice of law principles. (ECF No. 160 at 7). This court found that South Carolina law, as the law of the forum, was proper at the time because the place of the breach could not be determined based on the limited amount of discovery and “South Carolina was the only Blackbaud location specifically enumerated in the record.” *Id.* Notably, the court stated in that order that applying South Carolina law at this stage in the litigation³ and for the purpose of that specific motion, was

² This was originally assigned to Judge Michelle Childs, who ruled upon the motion to dismiss. The case was then reassigned to the undersigned district judge by the judicial panel on Multi-district litigation from upon Judge Childs’ elevation to the Court of Appeals.

³ See *Advanced Comm. Credit Int’l (ACI) Ltd. V. Citisculpt, LLC*, No. 6:17-cv-AMQ, 2018 WL 2149296, at *4 n.1 (D.S.C. May 10, 2018) (explaining that its choice of law finding was “not

proper and supported by the policy behind the *lex loci delicti* choice of law analysis.⁴ *Id.* at 7-9. However, the court made clear that additional facts learned in discovery might alter this analysis. *Id.* at 7.

Plaintiffs and Blackbaud agreed that additional briefing on choice of law was appropriate and agreed to brief the issue in advance of substantive motions practice after conducting more discovery. (ECF No. 228). The parties have filed their respective motions and responses on the choice of law analysis for the common law tort claims.

III. LEGAL STANDARD

The parties have stipulated to the application of South Carolina choice of law principles. (ECF No. 93). The court previously held that Plaintiffs common law claims for negligence, negligence per se, and invasion of privacy could proceed after Blackbaud moved to dismiss. (ECF No. 253-1 (citing ECF No. 160)). For tort claims, South Carolina uses the *lex loci delicti* analysis of the First Restatement of Conflict of Laws.⁵ “The *lex loci* doctrine is derived from the vested-rights approach which holds that a plaintiff’s cause of action ‘owes its creation to the law of the jurisdiction where the injury occurred and

intended to serve as a final determination of choice of law issues for all purposes” in the case if different facts developed during discovery).

⁴ “The long-time traditional reasons and arguments advanced for following, adopting, or adhering to the *lex loci* rule have been that it is relatively easy to apply, furnishes certainty and predictability of outcome (thus aiding litigants, lawyers, and insurers in assessing rights, liabilities, defenses, and damages), and, in addition is symmetrical—all persons injured, etc., in a single incident will have their rights adjusted by the same law.”

1 American Law of Torts § 2:9 (1970).

⁵ The goals of this approach are to “reduce forum shopping and increase predictability and uniformity” of result. *See* Yasamine J. Christopherson, *Conflicted About Conflicts? A simple Introduction to Conflicts of Law*, 21 S.C. LAW. 30, Sept. 2009, at 31.

depends for its existence and extent solely on such law.’” *Trahan v. E.R. Squibb & Sons, Inc.*, 567 F. Supp. 505, 508 (M.D. Tenn. 1983) (quoting *Winters v. Maxey*, 481 S.W.2d 755, 756 (Tenn. 1972)). Under the traditional or “vested-rights” approach, “the cause of action was considered to be created in the state of the tort, and the capacity to sue or immunity or defense was considered part and parcel of those rights.” 29 A.L.R.3d 603 (1970). Thus, under the traditional *lex loci delicti* test, the court applies the First Restatement’s reasoning where “the place of the harm is defined as ‘the state where the last event necessary to make an actor liable for an alleged tort takes place.’” *Wells v. Liddy*, 186 F.3d 505, 521 (4th Cir. 1999) (quoting RESTATEMENT (FIRST) OF CONFLICT OF LAWS § 377 (1934)).

The acts and events necessary to constitute a tort is a question of law that varies depending on the state. Restatement (First) of Conflict of Laws § 377 cmt. 1 (AM. L. INST. 1934). Applying the agreed upon South Carolina choice of law rules, the place of wrong is the location where the injury occurred, which is not necessarily the domicile of the plaintiff. *Rogers v. Lee*, 414 S.C. 225, 234, 777 S.E.2d 402, 407 (S.C. Ct. App. 2015). Further, South Carolina law provides “*lex loci delicti* is determined by the state in which *the injury occurred*, not where the results of the injury were felt or where the damages manifested themselves.” *Id.* at 231, 777 S.E.2d at 405. Therefore, the last event necessary for the tort to be a cognizable claim was the injury suffered by the Plaintiffs. Accordingly, the court must discern in which state the last act necessary to bring the claim occurred, *i.e.* the injury, and not where Plaintiffs may have felt the results of the injury or where the damages were manifested.

IV. DISCUSSION

As stated above, the main question presented in the choice of law briefing is where did the last act necessary for Blackbaud to potentially be liable for the common law tort claims occur? Determining where the last act necessary to identify that place of wrong is dependent on the elements of the specific tort at issue. *Cockrum v. Donald J. Trump for President, Inc.*, 365 F. Supp. 3d 652, 667 (E.D. Va. 2019). The torts claimed here include negligence, negligence per se, and invasion of privacy. The elements of negligence are duty, breach, causation, and damages. *Savannah Bank, N.A. v. Stalliard*, 400 S.C. 246, 251, 734 S.E.2d 161, 163-64 (2012). The last element necessary for a cognizable claim is damage to the plaintiff. *See Bank of Louisiana v. Marriott Int’l, Inc.*, 438 F. Supp. 3d 433, 443 (D. Md. 2020).

Plaintiffs have alleged that they “have been harmed and incurred damages as a result of the compromise of their PI in the data breach.” (ECF No. 77 at ¶ 555). Plaintiffs assert they have suffered injuries arising from Blackbaud’s negligence in the form of risk extortion (*id.* at ¶560), unauthorized disclosure of their PI to cybercriminals (*id.* at ¶ 563), loss of value in their PI (*id.* at ¶ 564), risk of future identity theft or fraud (*id.* ¶ at 566), and out-of-pocket mitigation expenses (*id.* at ¶¶568-70).

The damages from these claims stem from the same event—when the Plaintiffs’ PI was exposed.⁶ The initial damage occurred from the alleged risk of identity theft and the

⁶ Here, all three common law tort claims (negligence, negligence per se, and invasion of privacy) all depend on the point of intrusion as the last act necessary for potential liability. *See Cockrum v. Donald J. Trump for President, Inc.*, 365 F. Supp. 3d 652, 668-69 (E.D. VA 2019)(where the last

corresponding diminished value as a result of the cybercriminals' intrusion into Blackbaud's servers. The actual identity theft, emotional distress, and time and/or money spent to mitigate the harm all flow from the initial injury – the exposure of Plaintiffs' PI. Plaintiffs' alleged injury and the last event necessary for Blackbaud to be potentially liable in tort, was the cybercriminals' breach into the PI data servers. Thus, the court must determine where the data breach occurred.

Plaintiffs filed their motion on choice of law making the same argument that they made in the previous motion, that South Carolina law should apply as that is where Blackbaud's executives made the decisions which allowed improper access to the data. (ECF Nos. 252 & 253). Similarly, Blackbaud submitted the same argument in support of the position that each Plaintiffs' home state should apply as to the common law claims because the Plaintiffs' damages were felt in their respective home states. (ECF Nos. 254 & 255). Both sides also made a secondary and alternative argument that should the court find the primary choice of law suggestion was unfounded, then Massachusetts law would be appropriate. (ECF Nos. 253 & 254). Those arguments rest on the notion that Massachusetts was the state where the last act necessary took place because that is where the data servers were housed. *Id.* In continuity with the court's previous ruling and reasoning on the matter, Massachusetts law will apply as that is where the data breach occurred.⁷

act necessary for an invasion of privacy claim is the exposure of a plaintiff's personal information.).

⁷ Although the court used South Carolina law in the previous choice of law analysis, that was done based on the limited discovery the parties had conducted at the time and for purposes of that motion. (ECF No. 160). The court noted the decision was made with the reservation that the "point

Both Plaintiffs and Blackbaud maintain their respective positions that South Carolina or each Plaintiffs' state of residence should apply (respectively) to the common law tort claims. Neither parties' primary argument is persuasive. First, Plaintiffs suggest that South Carolina law should apply as that is where the cybersecurity related decisions were made. However, new discovery has illuminated the fact that the servers were located in Massachusetts and not South Carolina. Although some, if not most, of the decisions regarding the security were made in South Carolina by South Carolina based executives, that does not change the fact that the PI was stored on servers in Massachusetts.

Plaintiffs still contend that the last act necessary for Blackbaud to be liable in tort were the decisions it made regarding cybersecurity. That contention rests on the allegation that Blackbaud made the cybersecurity decisions from its headquarters in South Carolina. However, Blackbaud's decisions related to cybersecurity alone would not be the last act necessary for Blackbaud to potentially be liable. Those alleged decisions made in South Carolina may have contributed to the breach, but they were not the last act necessary to establish the cause of action. For Blackbaud to potentially be liable the cybercriminals would still need to breach the data servers. Plaintiffs' conclusion as to the law to be applied is incorrect because more events were required after Blackbaud made the cybersecurity decisions.

The cybercriminals intruded upon the information space by breaching the data servers located in Massachusetts, not in South Carolina. South Carolina's tort laws are not

of intrusion" factor was the nexus for the correctly applied law and that may change the state law to be applied once more discovery commenced. (ECF No. 160 at 7).

the proper choice upon which these common law claims should be litigated, because the point of intrusion, which ultimately caused Plaintiffs' damages, was in Massachusetts. Therefore, Massachusetts law will apply to the common law tort claims.

Likewise, Blackbaud's opinion that each Plaintiffs' state of residence should be the applicable law in which to litigate the common law tort claims also misses the mark. As the court previously stated in this order, South Carolina's choice of law rules dictate that where an injury occurs, not where the result of the injury is felt or discovered, is the proper standard to determine the last act necessary to complete the tort. Here, although Plaintiffs respective home states span the country, and many may have never been to the Northeast, the last act necessary for Blackbaud to be potentially liable occurred in Massachusetts once the cybercriminals breached the servers that housed the Personal Information.

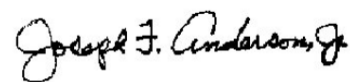
The court finds that the last act necessary in which Blackbaud could potentially be liable for the common law claims of negligence, negligence per se, and invasion of privacy occurred in the state in which the servers were located. Accordingly, the court will apply Massachusetts law regarding the claims for negligence, negligence per se, and invasion of privacy.

V. CONCLUSION

For the foregoing reasons, the court will apply Massachusetts law to the negligence, negligence per se, and invasion of privacy claims.

IT IS SO ORDERED.

June 28, 2022
Columbia, South Carolina



Joseph F. Anderson, Jr.
United States District Judge